UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/992,529	11/20/2001	C. Jay Wack	STSPT19CIP	1651

49691 7590 09/26/2005

IP STRATEGIES
12 1/2 WALL STREET
SUITE I
ASHEVILLE, NC 28801

EXAMINER	
DARROW, JUSTIN T	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 09/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/992,529	WACK ET AL.	
	Examiner	Art Unit	
	Justin T. Darrow	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *1-11,20 and 21* is/are allowed.

6)☒ Claim(s) *12-16 and 19* is/are rejected.

7)☒ Claim(s) *17 and 18* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 November 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 have been examined.

Priority

2. Acknowledgment is made that the instant application claims the benefit of the earlier filing date of provisional Application No. 60/249,451, filed 11/20/2000.

3. It is noted that the instant application is a continuation-in-part of Application No. 09/023,672, filed 02/13/1998, now U.S. Patent No. 6,885,747 B1. Under 35 U.S.C. 120, a claim in a U.S. application is entitled to the benefit of the filing date of an earlier filed U.S. application if the subject matter of the claim is disclosed in the manner provided by 35 U.S.C. 112, first paragraph, in the earlier filed application. See MPEP § 201.11 I. and *Tronzo v. Biomet*, 156 F.3d 1154, 47 USPQ2d 1829 (Fed. Cir. 1998). Priority is not granted for claims 1-21 with respect to Application No. 09/023,672, filed 02/13/1998, now U.S. Patent No. 6,885,747 B1 because the subject matter with respect to tagged data elements of independent claims 1, 10, 11, 12, and 20 is not disclosed in the manner provided by 35 U.S.C. 112, first paragraph, in the earlier filed application (see specification, page 5, lines 4-14).

Information Disclosure Statement

4. The information disclosure statements (IDSes) filed on 09/22/2004 and 03/08/2002 were filed before the mailing of the first Office action on the merits. The submission is in compliance with the provisions of 37 CFR 1.97(b)(3). Accordingly, the information disclosure statements are being considered by the examiner.

Drawings

5. New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because the drawings are informal. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 12-16 and 19 are rejected under 35 U.S.C. 102(b) as being anticipated by Lipner et al., U.S. Patent No. 5,557,765 A.

As per claim 12, Lipner et al. illustrates a process of transporting keying data corresponding to a cryptographic key comprising:

selecting the keying data corresponding to a cryptographic key (see column 12, lines 53-64; figure 7, step 710; generating a law enforcement access field (LEAF) corresponding to a session key (KS) from the selected key encrypted with a program public key and concatenated with a program identifier); and

sending the selected keying data to an intended recipient (see column 13, lines 8-9; figure 7, step 712; sending the law enforcement access field to a receiving program controlled by a recipient).

As per claim 13, Lipner et al. further states:

that the keying data comprises data needed to create the cryptographic key by a recipient (see column 14, lines 23-24; figure 17, step 1722; the law enforcement decryptor (LED) can obtain the session key (KS) by decryption the encrypted session key (EKS) in the law enforcement access field (LEAF)).

As per claim 14, Lipner et al. additionally specifies:

that the keying data comprises an algorithm identifier (see column 12, lines 57-58; figure 7, step 710; concatenating the encrypted session key (EKS) with a program unique identifier (UIP)).

As per claim 15, Lipner et al. then embodies:

that the keying data is encrypted before sending (see column 12, lines 58-59; figure 7, step 710; encrypting the concatenated data with a family public key).

As per claim 16, Lipner et al. next elaborates:

that the keying data is encrypted based on an encryption key, and the keying data comprises a key identifier corresponding to the encryption key (see column 12, lines 53-58;

figure 7, step 710; the session key is encrypted with a unique public key of a program with an identifier that is concatenated to the law enforcement access field).

As per claim 19, Lipner et al. also depicts:

formatting the keying data according to a cryptographic message syntax (see column 12, lines 59-60; the law enforcement access field is symbolized as [[KS]Kupub|UIP]Kfpub).

Allowable Subject Matter

8. Claims 1-11, 20, and 21 are allowed.

9. Claims 17 and 18 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

10. The following is an examiner's statement of reasons for allowance:

Claims 1-9; 10; and 11 are drawn to a cryptographic key split combiner, a process of creating a cryptographic key, and a process of cryptographically securing one or more respectively tagged data elements, respectively. The closest prior art, Hirsch, U.S. Patent No. 5,276,738 A, discloses a similar key split combiner and processes. Hirsch illustrates a cryptographic key split combiner, a process of creating a cryptographic key, and a process of cryptographically securing one or more respectively tagged data elements, comprising: a plurality of key split generators for generating cryptographic key splits (see column 1, lines 57-67); in which each of the key split generators includes means for generating key splits from seed data (see column 1, lines 49-54 and lines 62-64). However, they neither teach nor suggest that at

least one of the cryptographic key splits is based on at least one of the one or more respective tags. This particular limitation incorporated into independent claims 1, 10, and 11 renders claims 1-9; 10; and 11, respectively, allowable.

Claims 20 and 21 are drawn to a method of providing multi-level cryptographic security. The closest prior art, Lipner et al., U.S. Patent No. 5,557,765 A, discloses a similar method. However, this reference neither shows nor motivates generating a cryptographic key based upon the respective tag of a selected tagged data element (see column 12, lines 49-51; encrypting a data message M using a secret session key KS). This distinct step explicitly recited in independent claim 20 renders claims 20 and 21 allowable.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

11. The following is a statement of reasons for the indication of allowable subject matter:

Claims 17 and 18 are drawn to a process of transporting keying data. The closest prior art, Lipner et al., U.S. Patent No. 5,557,765 A, discloses a similar process. Although Lipner et al. describes that the keying data comprises an algorithm identifier (see column 12, lines 57-58; figure 7, step 710; concatenating the encrypted session key (EKS) with a program unique identifier (UIP)), this reference neither teaches nor suggests that the keying data comprises an encryption algorithm identifier corresponding to an encryption algorithm. This particular feature explicitly recited in dependent claims 17 and 18 renders them to have allowable subject matter.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Van Oorshot et al., U.S. Patent No. 5,850,443 A, describes data structure for an encrypted message with the encryption key for the message encrypted with a recipient's public key acting as a tag to allow the recipient access to the message

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (571) 272-3801, and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (571) 272-3799.

The fax number for Formal or Official faxes to Technology Center 2100 is 571-273-8300. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers transmitted by fax usually require three business days for entry into the application file and

consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to 571-273-8300 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only "**OFFICIAL FAX**" but also "**AMENDMENT AFTER FINAL**".

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (571) 272-2100.

September 23, 2005

Justin Darrow

JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100